

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the receiver and having

(1) means for associating said dispatch-related information with said element a1 by generating authentication-information comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

(2) means for securing at least part of said authentication-information against tampering of said sender and recipient.

65. A method for authenticating that certain information has been transmitted from a sender via a dispatcher to a recipient, comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said recipient, and said one or more information elements a2,...,an comprising dispatch-related information and comprise at least the following elements:

a2 - a time indication associated with said dispatch; and

a3 - information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient;

associating, by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, said dispatch-related information with said element a1 by generating authentication-information comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

securing, by said authenticator₂, at least part of said authentication-information against tampering of said sender and recipient.

66. A method of authenticating a dispatch and contents of the dispatch transmitted from a sender to a recipient, comprising the steps of:

receiving content data representative of the contents of the dispatch originated from the sender and being electrically transmitted to said recipient, and a destination of the dispatch;

providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

associating, by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

securing, by said authenticator₂, at least part of the authentication data against tampering of the sender and the recipient.

67. An authenticator for authenticating a dispatch and contents of the dispatch transmitted by or for a sender from a transmitting system to a receiving system for a recipient via an electronic communication network, comprising:

an input unit coupled to the communication network or to the transmitting system for receiving content data representative of the contents of the dispatch being electronically transmitted to said receiving system, and a destination of the dispatch;

means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

a processor for associating the content data with dispatching record data which includes at least said time related indicia and an indicia relating to the destination of the dispatcher and the contents of the dispatch; and

means for securing at least part of the authentication data against tampering of the sender and the recipient, the authenticator functioning as a non-interested third party with respect to the sender and the recipient.

68. An information dispatch system in an electronic communication network comprising;

a source transmitting system coupled to the electronic communicating network for sending a dispatch from a sender to a recipient;

a destination receiving system coupled to the electronic communication network for receiving the dispatch for the recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the recipient for authenticating the dispatch and contents of the dispatch transmitted from the source transmitting system to the destination receiving system, including:

(1) an input unit coupled to the communication network or to the source transmitting system for receiving content data representative of the contents of the dispatch being electronically transmitted to said destination receiving system, and a destination of the dispatch;

(2) means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

(3) a processor for associating the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

(4) means for securing at least part of the authentication data against tampering of the sender and the recipient.

69. A method of authenticating a dispatch and contents of the dispatch from a sender to a recipient, comprising the steps of:

electronically receiving content data representative of the contents of the dispatch originated from the sender, and a destination of the dispatch;

generating a paper document printout of said electronic content data to be dispatched to said recipient via a selected manual delivery service;

providing an indicia relating to a time of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

associating, by an authenticator functioning as a non-interested third party with respect to the sender and the recipient, the content data with dispatch record data which includes at least said time related indicia and an indicia relating to the destination of the dispatch, to generate authentication data which authenticate the dispatch and the contents of the dispatch; and

securing, by said authenticator, at least part of the authentication data against tampering of the sender and the recipient.

70. A certificate for attesting a dispatch and contents of the dispatch, comprising a representation of the following authentication data:

content data representative of the contents of a dispatch being electronically transmitted by a sender to a recipient; and

dispatch record data which includes at least an indicia relating to the destination of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and at least part of said authentication data being secured against tampering of the sender and the recipient, wherein the

authentication data are generated and secured by an authenticator functioning as a non-interested third party with respect to the sender and the recipient.

71. A method for verifying the authenticity of either of the contents, the time and the destination relating to a dispatch from a sender to a recipient, comprising the steps of:

providing a representation of either of said information elements;

verifying said representation for match with a representation of at least part of authentication data, said authentication data generated by an authenticator functioning as a non-interested third party with respect to the sender and the recipient and comprising a representation of the following information element: content data representative of the contents of the dispatch being electronically transmitted by the sender, and dispatch record data which includes at least an indicia relating to a time of the dispatch and an indicia relating to the destination of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and said authentication data being secured against tampering of the sender and the recipient.

72. A method according to claim 72 wherein the step of verifying includes verifying according to a verifiable digital signature verification procedure or according to a digital time stamping service verification procedure or a combination of both.

73. A certificate according to claim 70, wherein said authentication data is secured according to a digital signature or time stamping service scheme or a combination of both.--

REMARKS

The present application is a continuation of U.S. Application Serial No. 08/981,461, which was a national phase application of International Application No. PCT/IB96/00859. In the parent '461 application, a Final Action was issued on April 18, 2000. In response, applicants submitted a Request For Reconsideration And Amendment After Final ("the Request") on August 2, 2000. The Request was not entered. Nevertheless, after an Examiner Interview, applicants submitted a Supplemental Amendment After Final to implement certain